DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D.C. 20301

3 FEB 1977

U-019/DC

TO: Mr. E. H. Knoche
Acting Director of Central Intelligence
Washington, D. C. 20505

SUBJECT: DIA Presentation

1. Attached is a copy of the presentation I made to the Interagency Classification Review Committee.

2. It was carefully coordinated within the Intelligence Community and represents, I believe, a fair assessment of the issues related to the need for protection of national security information versus the public's right to know.

3. You might find this helpful in developing presentations along similar lines.

FOR THE DIRECTOR:

STAT

JOHN T. HUGHES
Senior Intelligence Advisor

1 Enclosure a/s

0516

Rtg	Office	INIT	Date
	D/DCI/IC		
	EA		
2	AD/DCI/IC	J	9 FEB 1977
1	EO	RV	9 Feb
	SA(Thomas)		
	SA(Showers)		
	CFI(Sec't)		
	NFIB(Sec't)		
	Ch, Spt Staff		
3	Ch, Registry	C/FICS	
	CH, OPP		
	P&PD		
	IHD		
	SECOM		
	CH, OPBD		
	DSG		
	PCEDD		
	PAD		
	CH, OPEI		
	Integ Staff		
	SIGINT Div.		
	IMAGERY Div.		
	HRD		
	PA&ID		

When circled - cy has been furnished.

Initialing, although there is little I need substantive on concerning what actions should be taken to ensure the principles are secured.

← I am sending copies to:
OPEI (SD - ID - PAID)
OPP (Secom)
AND MR. LANSDALE

OK
11 Feb 77

	UNCLASSIFIED	CONFIDENTIAL	SECRET

EXECUTIVE SECRETARIAT

Routing Slip

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	D/DCI/IC		✓		
4	DDS&T				
5	DDI		✓		
6	DDA		✓		
7	DDO				
8	D/DCI/NI				
9	GC				
10	LC				
11	IG				
12	Compt				
13	D/Pers				
14	D/S				
15	DTR				
16	Asst/DCI				
17	AO/DCI				
18	C/IPS				
19	DCI/SA				
20	D/EEO				
21					
22					
	SUSPENSE		Date		

Remarks:

25X1

Executive Secretary

8 Feb

Date

3637 (7-76)

1 DEC 1976

PROTECTION OF NATIONAL SECURITY INFORMATION

The invitation to address this symposium specified that I speak for the Intelligence Community on behalf of the need to protect selected national security information from unauthorized disclosure to the public. Before I discuss the basic issues, I would like to say three things in introduction.

First, although what I say does represent a fairly strong consensus for more openness within the Intelligence Community, I cannot "speak for" the Community as a whole. The subject of public disclosure is controversial, not only in the public sector, but also within the government.

Second, like many in the Intelligence Community, I firmly believe there can be compatibility between the public's right to know and the government's need to withhold selected national security information of which our foreign intelligence information is a special consideration. It must be remembered that the Intelligence Community collects, analyzes, and reports information on foreign powers in order to give U.S. policymakers the information they need to make vital decisions affecting the nation as a whole -- and, indeed, the free world. We in the Intelligence Community recognize that the general public also plays a role in policy development. The people themselves, their representatives in the Congress, and the elected and appointed members of the Executive Branch -- all need information of varying types and degrees in order to make or support sound decisions.

The third point to be made in introduction is that the Intelligence Community recognizes that preventing the unauthorized disclosure of truly important

secrets depends, to a fairly large degree, on keeping the number of those secrets relatively small. This supports the earlier thesis that there can be harmony between disclosure of essential information and secrecy, since disseminating such information not only informs the public, it also reinforces the security discipline necessary to protect truly sensitive and source revealing information.

With these thoughts in mind, I will now focus on three basic areas. First, the essential and continuing need for a security classification system to protect intelligence sources and methods, as well as other national security information. Second, the growing support for greater release of intelligence information to the American people to insure broadened awareness about national security issues of urgent concern. Third, some actions underway to increase public access and awareness while protecting vital national security information, especially that concerning intelligence collection sources and methods and analytical procedures.

Let me turn now to the first major theme, the need for protecting selected national security information from unauthorized disclosure. In doing so, I will concentrate on examples closely related to my own special area of interest -- intelligence collection sources.

What is that truly sensitive information that must be protected against disclosure? The Intelligence Community is primarily concerned about protecting the sources of its intelligence information and protecting certain analytical methods employed to develop meaningful findings and estimates. Everyone, I think, accepts the fact that a human agent with access to the secrets of a

foreign power, if identified, will be neutralized, and will no longer be able to give intelligence analysts, or the U.S. public, any useful information. The Intelligence Community believes that the need to protect source identity far outweighs any benefit to the public through explicit disclosure of a sensitive source. In fact, such a disclosure would be self-defeating to the very public who needs the intelligence products. Clearly, the public's right to know ought to include the right not to have intelligence sources negated through needless publicity about the identity of such sources.

Of course, a great deal of information these days is not obtained from spies or agents but from very sophisticated, highly technical means of intelligence collection. The effectiveness of these sophisticated collection systems can often, through unauthorized disclosure, be neutralized by a foreign power, sometimes as easily as a human agent. Preserving the flow of information from technical sources depends very largely on concealing what those sources are and how effectively they work. Clearly, by breaking an enemy communication code (as we did against the Japanese during WW II), we can obtain vital information on an enemy's plans and intentions. Once he learns we have broken that code, however, it is an easy matter for him to change the code, and thereby, either shut off that source of vital information or make our future collection and analytical efforts more difficult and costly.

There is another aspect of intelligence information and source protection which should be considered: that is the impact of accurate and timely intelligence on allocation of national resources to defense by the President and the Congress. We all recognize that maintaining U.S. military forces

as a credible deterrent in today's world is an undertaking which is becoming more and more costly. One of the contributors to growing costs is uncertainty -- uncertainty about the military capabilities of potential adversaries. If the U.S. leadership knew with greater precision the detailed Soviet plans for deployment and improvement of their strategic nuclear forces, the U.S. could design its own deterrent forces against a much narrower range of capabilities. Any unauthorized disclosures which lessen our collection capability would contribute to greater uncertainties or imprecisions in the quality of our intelligence information and could generate requirements for even larger defense expenditures to cover an even broader range of deterrent possibilities. If through disclosure of the intelligence sources we do have, and the consequent loss of vital information, the range of uncertainty is increased, then our weapons costs will probably go up.

Another aspect of the defense resources problem concerns the costs of intelligence collection systems themselves. You realize that the U.S. develops and operates some very sophisticated collection systems to get necessary information about foreign military capabilities which is not available from overt sources. You also recognize that the Soviet Union is a closed society which permits few overt sources to exist, and thus appreciate that this means the U.S. must employ expensive collection systems to get necessary information about Soviet military capabilities. Compromise of the vulnerable aspects of these expensive systems would not only deny us needed information, it could also force us into ever greater expenditures on new collection systems and processing techniques. Competition in armaments is expensive, but accurate

and timely intelligence helps keep the cost down. Competition in intelligence collection is also expensive, but good security -- protection of information about sources and methods -- helps keep the cost down in this realm, too.

Let me move to another major point about the need for security classification. Requests for disclosure of defense and foreign intelligence information are often accompanied by the comment that: "we are not asking the government about its sources, we just want to have the information -- to know the facts." In some instances, the facts can be provided. However, there are other facts which can only have come from a particular and sensitive sources, and disclosing those facts would automatically reveal the source. For this reason, the Intelligence Community must disguise some facts -- "sanitize" them as we say in our jargon -- so that the foreign target of our intelligence collection will not learr the source identity. Sanitization involves rounding off details, generalizing and, most important, combining individual raw items of information with other less sensitive information, thus making more difficult the foreign intelligence analyst's job in tracing the facts back to a particular source. Sanitization is never easy, and sometimes it is impossible. Unfortunately, when a fact cannot be effectively sanitized, it is hard for the Intelligence Community to explain or prove to the general public how a given fact reveals the source of that information. I think this particular problem is a major cause of many disagreements today, between those who argue for greater disclosure and those who argue for greater security. You often read a sensitive item in the papers which was published because neither the reporter nor his informant knew enough about sensitive intelligence

collection and processing methods to recognize how damaging that disclosure could be. The Intelligence Community in turn cannot explain publicly this relationship without making the loss of that source even more likely.

What I am saying here is that, to a degree, you cannot expect the Intelligence Community always to be prepared to explain publicly, in complete and convincing detail, why a particular item of information is sensitive, because the explanation itself may very well be sensitive. We must often ask the public's forbearance when we say that a certain item would reveal sensitive sources and methods. I feel the public understands this and wants to prevent disclosure of intelligence vital to national security.

I said in my introduction that there is a consensus in the Community these days toward more openness. Many have come to believe that some sources are not so easily jeopardized through disclosure as we once feared. Hence, many now believe that we can afford to risk disclosures which reveal some kinds of sources more than we once were willing to. We are trying to narrow our definition of what is a vulnerable source and to be more liberal in regard to dissemination of intelligence information from the least sensitive source.

We are working on this approach and making some progress, but just as there are some who are working hard toward this goal, there are others -- dedicated public servants -- who are not persuaded that the risk of security compromise is acceptable in many of these cases. Since an intelligence source once lost is seldom regained, we have to move prudently, and this is another area in which the public can be helpful. Compromises and leaks naturally generate

support for more restrictiveness. The more the public is willing to recognize that some intelligence sources are vulnerable and need protection, and not press for complete disclosure, the more progress we can make.

Up to this point, we have focused attention on the need to protect information about intelligence sources and methods. There are other kinds of information which need protection. Over the past 50 years, there has evolved a set of circumstances, including the threat of war, which justifies withholding certain defense-related information from the public sector and, thereby, from easy access by a potential adversary. In time of war or crisis, advance information concerning military plans could result in the defeat of major military operations. Even during peacetime, the disclosure of information about contingency military plans or data concerning certain aspects of U.S. military technology can assist foreign powers in coping more effectively or in developing countermeasures.

Let me give you some examples of the importance of keeping some kinds of defense-related information secret. Those of us who are intelligence collectors, have gained some insight into the value of information on foreign weapons systems and military plans. The kinds of things we collectors go out looking for on foreign powers, are precisely the kinds of things the U.S. has to keep secret as far as our own forces are concerned.

The first example has to do with missile guidance systems. You have all seen in the papers recently that the U.S. Navy was prepared to spend over a million dollars to recover a Phoenix air-to-air missile, along with the F-14 aircraft,

from the North Sea, in order to prevent its recovery by the Russians. This expenditure was justified by the fact that the effectiveness of the Phoenix hinges, to a considerable degree, on keeping some of its operating characteristics from a potential enemy. If these characteristics -- operating frequencies, coding devices, guidance logic -- are known to a potential enemy, he can design electronic countermeasures equipment which will seriously reduce its effectiveness. We are then placed in the position of having to change those characteristics, or design counter-countermeasures, which add immeasurably to the cost. We also lose time, which can mean a much reduced effective life for the operating system. If we are anxious enough to spend a lot of money to prevent physical recovery by a potential enemy, it is clear that we are not going to publish the detailed system characteristics in the newspaper to save them the trouble of having to collect the information. Classifying and withholding this kind of information contributes to the effectiveness of the weapon in combat, hence increases the likelihood that the U.S. will win an engagement in which the weapon is used. Conversely, disclosing the information will increase the likelihood that the weapon would be defeated and such an engagement won by a potential enemy.

Another example from recent news reports is instructive. Many of you, I am sure, have read in the press about recent proposals to restructure the military posture of the NATO forces in Central Europe, because of a belief that the Soviet Union is capable of a standing start offensive against the West. Such proposals may involve considerable expenditure of funds, and could affect the capability of the NATO powers to respond to a surprise offensive. This example is adduced to point up that precise knowledge of Soviet readiness,

and Soviet plans for an offensive in Europe, would permit the Western Allies to position their forces most effectively to counter an offensive, and with maximum resource efficiency. Not knowing those plans and that readiness forces us into difficult choices, it raises the chance of ineffectiveness or inefficiency in structuring our conventional force deterrent. The Soviet Union thus gains a real advantage by withholding from us information on their readiness and their plans. In exactly the same way, we seek an advantage by keeping from the Soviets (and unavoidably the U.S. public) detailed information on U.S. readiness and U.S. plans for defense of Western Europe.

Let me conclude this discussion of the needs for security classification with the observation that intelligence officers do not consider themselves the adversary of public affairs officers, newsmen, or citizens. By and large, intelligence officers are dedicated to dissemination of information -- which is acquired at such great cost and personal effort -- to the Congress and the public, where feasible, so that they can use it in effectively performing their role in the political process of this country.

Now let us turn to the second major portion of this discussion -- the high level awareness of the need to disclose selected national security information to the Congress and the public, and review some case histories of key releases.

I have been involved in three significant efforts by three Secretaries of Defense to disclose important national security information to the public

which was derived from sensitive sources. I'm sure there have been and will be others. A brief summary of the three illustrates how the government is broadening its efforts to inform the public about foreign military capabilitie

The first instance was the Cuban Missile Crisis of 1962. Once we had obtained direct evidence from photographic reconnaissance of Soviet strategic missiles in Cuba, President Kennedy decided that this threat to national security was so important to the security of the country that the people as well as the Congress needed to be fully informed. The objective was first to clearly establish that the Soviets had installed the missiles, and later that the Soviets had removed all strategic weapons from the Island and returned them to the Soviet Union. Initially, a series of classified presentations were provided to the Congress. Subsequently, Secretary McNamara sponsored a televised press conference at which aerial photography, acquired during the Crisis, was displayed and explained to the public. To my knowledge, this was the first revelation of our U-2, quality photography and of our comprehensive knowledge of the nature of the Soviet presence.

The second and more recent example resulted from Secretary Schlesinger's belief that the Congress and the public should be informed of the hard evidence on the growing Soviet presence in Somalia and the implications for U.S. Indian Ocean policy. In 1974, the Secretary of Defense gave a series of presentations to the Congress using sensitive imagery of Somalia and including many facts related to the imagery which we had initially learned through other sources. Concurrent arrangements were also made to provide a presentation before an open Senate session and to release copies of the photographs themselves to the public.

The third example is one in which DIA is now engaged. At the direction of Secretary Rumsfeld, an unprecedented series of classified presentations has been given to the Congress about current Soviet military capabilities and trends, using information derived from extremely sensitive sources. The Congress published an unclassified version in the Congressional Record.

Let me make one very important point about these three examples of public disclosure. All of the briefings were primarily classified and addressed first to the Congress. This reflects a recognition that, even though sources may be vulnerable and all information cannot always be revealed to the general public, it must be revealed to the public's elected representatives in the Congress. Where we can declassify, we will. Where we cannot, we must ensure that the Congress is always informed.

I would like to emphasize that the most difficult problem we deal with in these briefings is how to get the hardest possible evidence (which means unfortunately the most source-revealing) before the public. In this instance, I can tell you that we are still uncertain as to how open we can be without endangering these critically important sources. I can say that we are carefully and gradually working towards what I think will be a new more liberal information release policy, with many implications for all of the government in the future.

Now, for the last of the three major subjects, let me describe some specific proposals to increase public access and awareness, which are currently being discussed within the Intelligence Community.

First, we need to be much more disciplined in the way we write intelligence reports. We must make the greatest possible effort to use highly sensitive material only when necessary, and then have it clearly identified so that any sanitization of reports for public release (either on our own initiative or in response to FOI requests) will not jeopardize sensitive information and be more timely. Some things we are looking at in this area are: the problem of "inherited classification" (classifying a document because of the documents which preceded it rather than its actual substance); the need for greater differentiation between reports written for intelligence analysts who need source details and users of intelligence who need the substantive results of analysis.

Further, we are making a major effort to reduce to some degree the use of special compartmentation and dissemination restrictions, which hinder downgrading and declassification.

Second, we need more emphasis in the Intelligence Community on policing disclosure procedures. The mechanisms which exist inside the Intelligence Community to prevent overclassification are in a more rudimentary state than those outside the Community. In this area, we can learn from you.

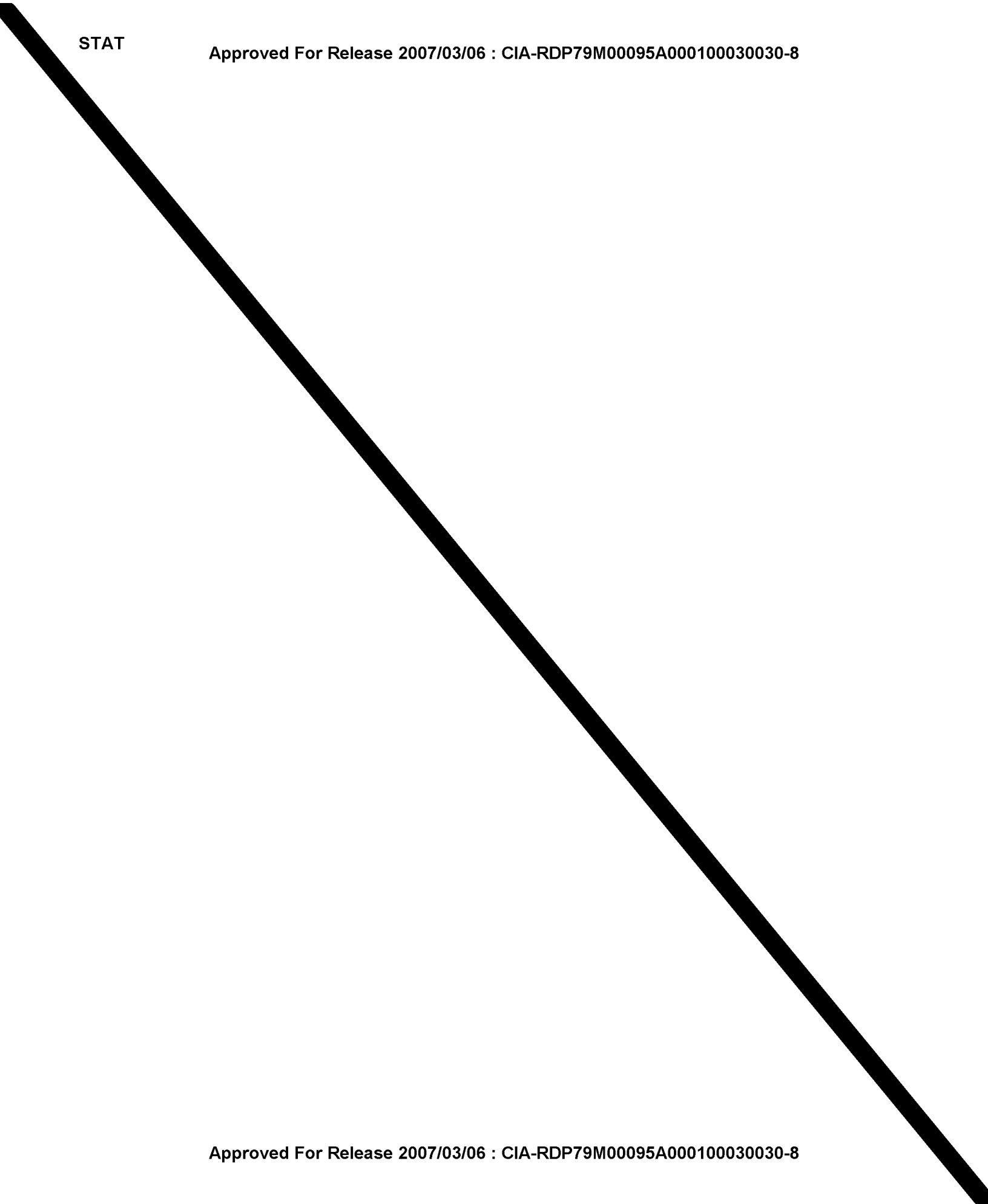
Third, we are thinking hard about formalizing public disclosure arrangements. We are considering the need to establish mechanisms within the major

intelligence elements for regular, routine, and more frequent preparation or release of unclassified reports.

In summary, I have talked first about the reasons for keeping sensitive national security information secret; second I have cited some examples in which Defense has disseminated source-revealing information to the public while maintaining essential security; and third I have described specific steps in progress or under consideration towards improving the balance between secrecy and disclosure.

I think it should be clear to any reasonable person that certain information must be protected against disclosure, in order to ensure that the flow of vital intelligence about foreign powers is able to continue. Other national security information also must be protected against disclosure in order to make more difficult a potential enemy's efforts to counter our military plans, operations and weapons systems.

While vital intelligence information must be protected, I believe we are doing much to maximize the flow of information to the Congress and the public, and can and will do more. Fundamentally, I believe a balance between secrecy and disclosure can be struck which will meet both goals.



Approved For Release 2007/03/06 : CIA-RDP79M00095A000100030030-8